Голові разової спеціалізованої
вченої ради PhD 17107
Хмельницького національного
університету
доктору технічних наук,
професору Сергію ЛИСЕНКУ
29016, м. Хмельницький,
вул. Інститутська, 11

ВІДГУК
ОФІЦІЙНОГО ОПОНЕНТА

на дисертаційну роботу Віжевського Петра Володимировича
на тему «Методи та засоби виявлення і запобігання витоку даних в корпоративних мережах згідно еволюційних алгоритмів», подану на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 122 Комп'ютерні науки

1. Актуальність теми дисертації.

Сучасні корпоративні мережі обробляють великі обсяги конфіденційної інформації, а її витік призводить до прямих фінансових втрат, регуляторних санкцій і репутаційної шкоди. Значна частина інцидентів витоку пов'язана не із зовнішнім зломом, а з діями внутрішніх користувачів, які мають легітимний доступ до даних і використовують дозволені канали передачі. Це робить системи запобігання витокам даних (ЗВД) обов'язковим компонентом корпоративної безпеки.

Разом із тим наявні ЗВД-системи здебільшого спираються на статичні правила контентного аналізу, які адміністратор має налаштовувати і підтримувати вручну. У динамічному середовищі з хмарними сервісами, гібридною роботою та постійно змінюваними форматами документів такі правила швидко застарівають, що проявляється як у пропущених інцидентах, так і в значній кількості хибних тривог. Спроби додати адаптивності за рахунок непрозорих моделей машинного навчання натомість ускладнюють аудит рішень системи.

Перспективним підходом є використання еволюційних алгоритмів, які дозволяють автоматично формувати та перенавчати компактні набори правил, придатні для експертної перевірки, а також оптимізувати конфігурацію індивідуальних поведінкових профілів користувачів. При цьому актуальними залишаються питання виявлення дрейфу концепції без оперативних міток істинності та узгодження всіх компонентів у межах єдиної формальної моделі.

Таким чином, тема дисертації, присвячена розробленню методів і засобів виявлення та запобігання витоку даних у корпоративних мережах на основі еволюційних алгоритмів, є актуальною і відповідає предметній області спеціальності 122 Комп'ютерні науки.

2. Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційне дослідження виконувалось у рамках науково-дослідної тематики Хмельницького національного університету, зокрема держбюджетної науково-дослідної теми № 1Б-2026 «Система забезпечення стійкості до витоку конфіденційної інформації в корпоративних мережах в умовах впливів комп'ютерних атак» (номер державної реєстрації 0124U001214), в якій автор дисертації є виконавцем.

3. Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни.

Наукова новизна результатів дисертаційного дослідження полягає в наступному:

1) удосконалено модель процесу запобігання витокам даних, яка, на відміну від наявних описових підходів з ізольованим розглядом компонентів ЗВД-системи, об'єднує моделі витоку, корпоративного середовища та даних у єдиній формальній схемі із чітко визначеними точками прикладення адаптивних механізмів, що дає змогу узгоджено проєктувати класифікацію документів, поведінкове профілювання та адаптацію політик як складники одного процесу, а не набір незалежних інструментів;

2) вперше розроблено метод класифікації документів за рівнем конфіденційності на основі генетичного алгоритму, особливістю якого є хромосомне кодування продукційних правил у поєднанні з регуляризацією складності моделі та, на відміну від жадібної індукції правил методом послідовного покриття (CN2, RIPPER) і від генетичного відбору правил із наперед сформованої бази знань, глобальний еволюційний пошук цілісних наборів правил безпосередньо в просторі ознак політик безпеки, що дає змогу отримувати компактний, придатний для аудиту та безпосередньої експертної інтерпретації набір правил із конкурентною якістю розпізнавання і за потреби відновлювати виявлення нового типу критичних ідентифікаторів одним дописаним експертом правилом без залучення розмічених прикладів;

3) вперше розроблено метод еволюційної адаптації політик ЗВД за умов дрейфу концепції, особливістю якого є детектор змін на основі підтвердженого багатоознакового статистичного тесту, стійкого до поодиноких хибних спрацювань, який, на відміну від класичних детекторів на потоці помилок

класифікатора (ADWIN, DDM, EDDM, KSWIN), працює безпосередньо з розподілом вхідних ознак і не потребує оперативних міток істинності, у поєднанні з еволюційним перенавчанням політик, яке, на відміну від інкрементних і ансамблевих схем адаптації, зберігає інтерпретовану структуру набору правил, що дає змогу суттєво зменшити кількість хибних тривог за повного виявлення справжніх змін і втримати точність класифікації в нестаціонарному потоці;

4) набув подальшого розвитку метод поведінкового профілювання користувачів, який, на відміну від глобальних методів виявлення аномалій з єдиною моделлю нормальної поведінки для всієї сукупності користувачів, ґрунтується на індивідуальному адаптивному профілі кожного користувача з генетичною оптимізацією його конфігурації та ваг ознак, що дає змогу точніше виявляти внутрішніх порушників у межах реалістичного бюджету тривог.

Наукові положення, висновки і рекомендації дисертаційної роботи Віжевського Петра Володимировича обґрунтовані коректним використанням математичного апарату та підтверджені експериментальними дослідженнями. При розв'язанні поставленої науково-прикладної задачі використано теорію множин для формалізації моделі даних, категорій конфіденційності та ознакового простору документа; теорію графів для побудови моделі корпоративного середовища з рольовим доступом, зонами безпеки і точками контролю; теорію ймовірностей та математичну статистику для ризик-моделі інциденту витоку, детектора дрейфу на основі критерію Колмогорова-Смирнова та оцінювання результатів; методи машинного навчання й еволюційної оптимізації для розроблення методів класифікації документів, адаптації політик і поведінкового профілювання.

Достовірність результатів забезпечена проведенням експериментів на загальновідомих відкритих наборах даних (ai4privacy, 20 Newsgroups, CERT Insider Threat r4.2, Electricity, INSECTS, RandomRBF), застосуванням стандартних метрик якості класифікації і преквенціального оцінювання, порівнянням із відомими методами та алгоритмами, використанням перехресної перевірки та довірчих інтервалів для основних показників. Наукові положення логічно випливають з отриманих результатів, а окреслені автором межі застосовності методів (підрозділ 4.4) додають висновкам обґрунтованості.

Отже, в дисертаційній роботі поставлене наукове завдання виконано, а здобувач оволодів методологією наукового дослідження.

4. Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності.

За своїм змістом дисертаційна робота здобувача Віжевського Петра Володимировича відповідає Стандарту вищої освіти зі спеціальності 122 Комп'ютерні науки для третього (освітньо-наукового) рівня вищої освіти та освітньо-науковій програмі Хмельницького національного університету за цією спеціальністю. Дисертаційна робота є завершеною науковою працею і свідчить про особистий внесок здобувача у розвиток методів захисту інформації в корпоративних мережах.

Розглянувши дисертаційну роботу, можна зробити висновок, що вона є результатом самостійних досліджень здобувача і не містить елементів плагіату та запозичень. Використані результати і тексти інших авторів мають належні посилання на відповідні джерела.

5. Практичне значення отриманих результатів.

Результатом дисертаційної роботи є програмний комплекс ЗВДЕАГА, реалізований мовою Python у модульній архітектурі, що відповідає розробленій формальній моделі та об'єднує класифікацію контенту на продукційних правилах, поведінкове профілювання користувачів, виявлення дрейфу та еволюційну адаптацію політик. Комплекс зареєстровано як об'єкт авторського права. Експериментально показано, що класифікатор досягає F1-міри 0,826 на корпусі документів з персональними даними за приблизно п'яти правил, поведінковий профіль виявляє інсайдерів у 2,5 раза точніше за глобальні детектори аномалій, правило підтвердження детектора дрейфу скорочує кількість хибних тривог у 3,5 раза, а еволюційна адаптація підвищує преквенціальну точність на реальних потоках на 6,6-8,0 %. Сформульовано рекомендації щодо під'єднання компонентів комплексу до поштового чи проксі-шлюзу та SIEM-системи.

Теоретичні та практичні результати дослідження впроваджені в ТОВ «ІТТ» (м. Хмельницький, акт від 30.06.2026), ПП «Авіві» (м. Хмельницький, довідка від 29.06.2026), а також в освітньому процесі Хмельницького національного університету (акт від 26.06.2026) при викладанні дисциплін на кафедрі комп'ютерної інженерії та інформаційних систем для здобувачів спеціальності F7 Комп'ютерна інженерія, зокрема в курсах «Безпека та захист комп'ютерних систем» і «Методології забезпечення якості, надійності, гарантоздатності та безпеки комп'ютерних систем та мереж».

6. Мова та стиль викладення результатів.

Дисертаційна робота написана українською мовою, логічно та на належному науковому рівні з використанням усталеної термінології. Матеріал

викладено послідовно, доступно для сприйняття, формальні положення супроводжуються поясненнями позначень і числовими прикладами.

Дисертаційна робота складається з анотації, змісту, переліку умовних скорочень, вступу, чотирьох розділів, висновків, списку використаних джерел та семи додатків. Повний обсяг роботи становить 231 сторінку друкованого тексту, з них анотація займає 11 сторінок, зміст 2 сторінки, перелік скорочень 1 сторінку, вступ, розділи та висновки викладено на с. 15-199, список зі 137 використаних джерел займає 15 сторінок, додатки 17 сторінок. Дисертація містить 13 рисунків та 21 таблицю.

Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

7. Оприлюднення основних наукових результатів дисертаційної роботи.

За результатами дисертаційного дослідження опубліковано 10 наукових праць, у тому числі 5 статей у наукових фахових виданнях України категорії Б, 4 праці у матеріалах міжнародних наукових конференцій, з яких 2 опубліковано у виданнях, що індексуються наукометричною базою Scopus, а також одержано свідоцтво про реєстрацію авторського права на комп'ютерну програму «Програмний комплекс запобігання витоку даних з еволюційною адаптацією на основі генетичних алгоритмів (ЗВДЕАГА)» (№ 144040 від 04.03.2026).

Основні положення та результати дисертаційної роботи доповідались і обговорювались на міжнародних наукових конференціях та семінарах: 5th International Workshop on Intelligent Information Technologies and Systems of Information Security (IntelITSIS-2024, м. Хмельницький, березень 2024 р.); 14th IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT 2024, м. Афіни, Греція, 2024 р.); 1st International Workshop on Intelligent & CyberPhysical Systems (ICyberPhyS 2024, м. Хмельницький, червень 2024 р.); Modern Data Science Technologies Doctoral Consortium (MoDaST 2025, м. Львів, червень 2025 р.).

Опубліковані праці відображають повноту викладу результатів дисертаційної роботи. Наукові результати, подані в дисертації, повністю висвітлені у публікаціях здобувача, у яких дотримано принципів академічної доброчесності.

8. Недоліки та зауваження до дисертаційної роботи:

1. В описі наборів даних у підрозділі 4.1 (с. 176-178) для текстових корпусів, журналів активності користувачів і потокових даних не зазначено, яку саме задачу ЗВД і які особливості корпоративного середовища відтворює

кожний набір, тому роль окремих наборів у спільній програмі експериментів простежується лише за контекстом підрозділу 4.2.

2. Практичні рекомендації та межі застосовності методів у підрозділі 4.4 (с. 193-195) викладено в описовій формі. Зокрема зазначено, що для суто тематичної конфіденційності правила доцільно поєднувати з ансамблевою або лінійною моделлю в гібридній схемі. Систематизованого зіставлення методів за придатними типами даних, умовами використання та випадками поєднання з іншими засобами аналізу в роботі немає, що ускладнює вибір конфігурації ЗВД-системи для конкретного середовища.

3. Вплив ширини вікна допуску на облік виявлених змін і хибних тривог детектора дрейфу зазначено в описі протоколу (с. 178) лише словесно. Результати на с. 186-187 наведено для однієї ширини вікна, тому чутливість підсумкових показників детектора до цього параметра за матеріалами роботи оцінити не можна.

4. Приклад доповнення політики правилом для нового типу ідентифікатора (таблиця 4.5, с. 183) обмежено одним типом ідентифікатора. Випадок одночасного додавання правил для кількох типів ідентифікаторів і спосіб перевірки того, що нові правила не охоплюють документи без конфіденційних даних, у роботі не розглянуті.

5. Обчислювальні витрати методів порівняно з базовими алгоритмами оцінено, а еволюційне перенавчання рекомендовано виконувати на окремому обчислювальному ресурсі зі збереженням чинної політики до завершення валідації нової. Водночас у підрозділі 4.3 (с. 191-193) не наведено затримки обробки окремого документа, пропускної здатності комплексу та тривалості циклу перенавчання із зазначенням конфігурації обладнання, тому вимоги до обчислювальних ресурсів під час розгортання системи за матеріалами роботи не визначено.

6. Рекомендації щодо під'єднання комплексу до поштового або проксі-шлюзу та SIEM-системи (с. 192-193) подано на рівні схеми без прикладу інформаційного обміну. Склад вхідної події та спосіб передавання рішення ЗВД-системи суміжному засобу захисту не описано.

Але зазначені зауваження не є принциповими, істотно не впливають на зміст дисертаційної роботи та не знижують її наукової та практичної цінності.

9. Висновок про дисертаційну роботу.

На основі викладеного вище вважаю, що дисертація Віжевського Петра Володимировича на тему «Методи та засоби виявлення і запобігання витоку даних в корпоративних мережах згідно еволюційних алгоритмів», що подана на здобуття ступеня доктора філософії, є завершеною самостійною науковою

працею, у якій отримано нові науково обґрунтовані результати, що в сукупності розв'язують актуальну науково-прикладну задачу підвищення ефективності виявлення та запобігання витокам конфіденційної інформації в корпоративних мережах. За актуальністю, науковою новизною, практичною цінністю, змістом та оформленням дисертація відповідає вимогам пп. 6, 7, 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого постановою Кабінету Міністрів України від 12 січня 2022 р. № 44 (зі змінами, внесеними згідно з постановами Кабінету Міністрів України № 341 від 21.03.2022, № 502 від 19.05.2023, № 507 від 03.05.2024), а її автор, Віжевський Петро Володимирович, заслуговує на присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 122 Комп'ютерні науки.

Офіційний опонент,
доктор педагогічних наук, кандидат технічних наук,
професор, професор кафедри кібербезпеки
та математичного моделювання
Національного університету
«Чернігівська політехніка» Юлія ТКАЧ

15.10.2026 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Чернігівська політехніка»
ВІДДІЛ КАДРІВ

Підпис Ю.М. Ткач
засвідчую
начальник відділу кадрів
10 2026 р.